Journal of Technology Law & Policy

Volume 2 | Issue 1 Article 4

September 1996

The Genie Let Loose: Ineffectual Encryption Export Restrictions and Their Deleterious Effect on Business

Doug Masson

Journal of Technology Law & Policy
Volume 2 Fall 1996 Issue 1
Published by Students at the University of Florida College of Law

Return to Table of Contents | Comment on this Article

The Genie Let Loose: Ineffectual Encryption Export Restrictions and Their Deleterious Effect On Business

by Doug Masson [1]

Cite as: Doug Masson, *The Genie Let Loose: Ineffectual Encryption Export Restrictions and Their Deleterious Effect On Business*, 2 J. TECH. L. & POL'Y 3, <http://journal.law.ufl.edu/~techlaw/2/masson.html> (1996).

Introduction

{1} As digital networks expand, accelerate, burrow further into the framework of our lives, and become ubiquitous and generally indispensable, the methods by which we allow access to our individual slivers of the Global Information Infrastructure (GII) escalate to considerable importance. Specifically, the course of development and distribution of encryption technology is an obvious factor in how secure the networks will be, in how United States businesses will fare in the GII, in how governments interact with malefactors and each other, and in how private the individual can make her life, including, but not limited to, the level of her ability to determine who she will include in her exercise of First Amendment liberties.

{2} Of critical importance in the emergence of widely available encryption is the status of export laws restricting, regulating, and criminalizing the export of high quality encryption software. These laws classify encryption software as restricted items of trade at best and as munitions at worst. The laws were passed during the Cold War in an attempt to slow enemy countries' access to technology. It is a reasonably simple concept; primarily, an enemy's possession of encryption capabilities makes it harder for us to spy on them, and, secondarily, if an enemy possesses our encryption techniques, it makes it easier for them to figure out ways to spy on us.

{3} The peculiar importance of export laws stem from the global nature of information in general and the GII in particular. First, there is a need for standards; if an encryption program does not yet exist and is, in fact, being actively discouraged in a foreign country, it cannot be used in commerce with companies in that country and, if the program cannot be used in commerce with foreign countries, there is a strong possibility that, for reasons of efficiency, it will not be used domestically. This is especially true if commerce becomes so globalized that one is just as likely to trade with someone halfway around

the world as one is to trade with someone across town. With information as a commodity, such trade is not only entirely possible, it is probable. Second, networks are likely to become the primary means of distributing software, particularly software which is intended to be made widely available. The fact that networks used domestically are easily accessible from foreign countries means that strong encryption which is legal and desirable for the use of citizens cannot be distributed effectively or efficiently because the same networks which would enable distribution domestically are accessible by foreigners and, therefore, anyone who made encryption available via these networks would run afoul of U.S. munitions laws and export restrictions.

{4} In order to understand this issue, this paper will describe encryption generally, describe the export laws by looking at their requirements and justifications, describe the objections and positions of U.S. businesses, primarily from the software industry, with regard to these restrictions, describe the government's attempt at a solution to the export impasse, primarily by looking at the Clipper debate, and, finally describe the problems related to providing widespread, high quality encryption software domestically caused by the export restrictions, primarily by looking at the matter of Phil Zimmerman and his encryption program "Pretty Good Privacy."

I. A GENERAL DESCRIPTION OF CRYPTOGRAPHY

{5} Cryptography has been in use in one form or another for a very long time; Julius Caesar used a simple system whereby every letter was to be replaced by a letter three places behind the original letter in order to decrypt the message. [2] So "OBQOBXQ" becomes "RETREAT." The cipher or algorithm is the function used for encryption or decryption, in Caesar's example, it is a substitution function based on the number three; three being the key to the simple substitution algorithm.

{6} Caesar's was, of course, a very simple cipher, making the spy ciphers in cereal boxes appear complex by comparison. Things have changed dramatically since then. Modern algorithms have key lengths ranging in size from 40 to 128 bits. The difficulty of cracking a code by "guessing" the correct key is approximately proportional to the number of possible key values. Since each bit contains two possibilities (digital bits consisting of either a one or a zero), an eight bit key has 2 to the 8th power possibilities or 256 possible keys. Therefore, the strength of an encryption algorithm, as a general rule, grows exponentially with the number of bits available to it. [3]

{7} Essentially, there are two kinds of encryption systems that are used widely, "secret-key" systems and "public-key" systems. In a secret-key system, the encryption key and the decryption key are the same. In Caesar's system, the key is moving each letter three places in the alphabet. This system requires both the sender and the receiver to possess the key in order to communicate which, in turn, means that a secure system must exist by which to exchange such keys; this has traditionally been the weak link in secret-key systems. [4]

{8}The most popular secret-key algorithm in use today is the Data Encryption Standard (DES) invented by IBM in the mid-1970's with assistance from the National Security Agency (NSA). [5] Banks and financial institutions have since standardized the 56 bit secret-key algorithm for electronic funds transfers and other financial information. Though the technical details of DES and products incorporating DES are available and produced world-wide, exports of products using DES for data encryption are not allowed except to financial institutions or to subsidiaries owned at least 51% by U.S. companies. [6]

{9} RC2 and RC4 are "variable-key-size" ciphers which means that developers can make the keys long or short; when used with longer keys, they are alternatives to DES. In 1992, the Software Publishers

Association (SPA) reached an agreement with the government to allow export of products using these algorithms so long as their key size did not exceed 40 bits (DSA uses 56 bits), and, consequently, foreign customers have refused to accept such products as replacements for DES. [7]

{10} Public-key encryption was invented in the mid-1970s by two Stanford University scientists. They did this through the use of two mathematically related keys. Although they are a matched pair, it is infeasible to compute one key through the use of the other. Therefore, gone is the requirement that sender and receiver share a common key. Instead, it is possible for the sender to have a public key which is published in a directory while keeping his own private key. Ira S. Rubenstein describes a transaction taking place using the RSA public-key system as follows:

- {11} Imagine that Alice wants to send Bob an encrypted e-mail message. She looks up Bob's public key in a public-key directory. To send Bob a private message, she scrambles her e-mail with Bob's public key. Bob then decrypts Alice's message using his private key. The result: so long as Bob keeps his private key private, no one else can read Alice's message to him.

  {12} Alice can also digitally sign her message to Bob. She does so by encrypting the message with her own private key. Bob receives the message and looks up Alice's public key in the directory. If Bob can decrypt the message using Alice's public key, this confirms the mathematical relationship between the two keys. If Alice's public key does not decrypt the message, Bob knows that the message purportedly from Alice was not signed with Alice's key or that someone altered the message during transmission. [8]

{13} RSA, named after the initials of its three inventors (Ronald Rivest, Adi Shamir, and Leonard Adelman), is the most popular public-key encryption algorithm and is a de facto worldwide standard for digital signatures and privacy-enhanced e-mail. The algorithm for the RSA public-key system is freely available abroad and exports of products using RSA for digital signatures are permitted regardless of key size, but exports of software incorporating RSA is tightly restricted when used for privacy-enhancing data encryption. [9]

II. ENCRYPTION EXPORT LAWS

{14} During the Cold War, the United States sought to restrict items which were specifically designed, developed, configured, adapted, or modified for military application (defense articles) [10] as well as those items which were primarily useful for civilian purposes but which could be bent to military purposes, known as "dual use" items in the relevant parlance. [11] In furtherance of this objective, jurisdiction over the export of defense articles was given to the Office of Defense Trade Controls (DTC). These defense articles are listed on the U.S. Munitions List (USML) which is part of the International Traffic in Arms Regulations (ITAR). [12] "Information Security Systems and equipment, cryptographic devices, software, and components specifically designed or modified therefore" including "cryptographic systems or software with the capability of maintaining secrecy or confidentiality of information" is controlled by Category XIII(b) of the USML. [13]

{15} Dual-use encryption items fall into an exception, or, more properly, a frequently exercised waiver, to DTC's jurisdiction. DTC does not exercise jurisdiction over technical data that qualifies for the "public domain," [14] nor does it exercise jurisdiction over certain software DTC has agreed to transfer to the Commerce Department sometimes categorically, and sometimes on a case-by-case basis. Transferred encryption software falls under the jurisdiction of the Commerce Department's Bureau of Export Administration (BXA) which controls the export of dual use items. [15]

{16} For someone who desires to export encryption products, it is desirable to get one's product transferred to BXA jurisdiction because otherwise export will have to be licensed as a munition under ITAR. These munition licenses require an individual review for each end-user, there are no general licenses, and DTC will not approve licenses for products destined for communist, former communist, and terrorist nations. [16]

{17} The primary way in which to get transferred to BXA jurisdiction is to get a favorable Commodity Jurisdiction determination (CJ) CJ transfers fall into three main categories: automatic transfers, specifically enumerated in Category XIII(b)(1); expedited transfers of mass market software programs meeting specified requirements; and transfers based on a case-by-case review. [17]

- **A. Automatic Transfers**

{18} If cryptographic equipment performs any of the following functions and no others, it is automatically transferred from DTC to BXA, furthermore, the ITAR no longer even requires a statement from DTC verifying the transfer: 1) decryption only for copy-protected software; 2) bank or money transactions; 3) cryptographic processing using analogue techniques in certain radio and fax equipment; 4) certain personalized smart cards; 5) access control devices such as ATMs 6) data authentication; 7) fixed data compression or coding techniques; 8) set top decoders; 9) anti-virus software. [18]

- **B. Expedited Transfer of Mass Market Software**

{19} In 1992, DTC set up procedures to speed up the transfers of mass market software into BXA jurisdiction. "Mass market software" is defined as computer software that is available to the public via sales from stock at retail selling points, by means of over-the-counter transactions, mail order transactions, or telephone transactions. Such software must be designed for installation by the user without further support of substance from the supplier. Expedited review means that a determination will be made within fifteen days; furthermore, if all of the expedited review criteria are met and the software uses RC2 or RC4 algorithms of 40 bits or less, the exporter is entitled to a seven day review. [19]

{20} This rule provides a relatively convenient procedure for licensing software which meets the criteria; however, a general rule of thumb is that algorithms exceeding 40 bits will not qualify for expedited review. [20] C. Case by Case Review Certain mass market software products are eligible for jurisdiction transfer by means of a case by case review if 1) they are designed to run on microcomputers; 2) they employ "non-standard cryptographic algorithms, not of strategic value;" and 3) encryption is not the primary function. [21] Though neither BXA, DTC, nor NSA have ever explained what is meant by "non-standard" or "non-strategic" and though DTC does not publish licensing decisions, "it is generally understood that DTC will not approve licenses for DES-based encryption products except for financial institutions (and such approvals are generally restricted to financial transactions) or subsidiaries of U.S. companies." [22] NSA review of encryption using products under the case by case procedure could be quite extensive so exporters have a strong incentive to meet the expedited review guidelines, including the 40 bit limitation, in order to avoid lengthy delays.

{21} Once encryption products are transferred to BXA jurisdiction, if they are designed for installation by the user without further substantial support by the supplier, sold from stock at retail selling points, and publicly available products (which are the only products which fit within the scope of this paper, concerned as it is with businesses who presumably wish to sell their products widely as well as with the everyday individuals who make up the public to whom these products must be available), then they are almost always eligible for a general license, making them exportable to all destinations except for the

pariah nations of North Korea, Cuba, Libya, Iraq, Serbia, Montenegro, Iran, and Syria. [23]

{22} There are, therefore, many administrative hurdles which must be cleared in order to be permitted to export products employing encryption. The primary hurdle is avoiding DTC jurisdiction so as to be able to license one's products generally rather than having to obtain licenses for each end-user, and, the primary way to do this is to keep one's algorithm under 40 bits. Violating the export restrictions can result in a maximum criminal penalty of $1 million and ten years in prison [24] or a maximum civil penalty of $500,000 and a three year export ban. [25]

{23} The justifications for these bans tend to be inadequate when they are justified at all. The NSA, the agency primarily responsible for export restrictions, is fairly tight lipped about its rationale for maintaining the export restrictions; this should be expected to a certain extent, since it was only recently that the NSA admitted its existence at all. However, according to a report by the Association for Computer Machinery (ACM), the goals of U.S. export restrictions are: (i) to limit foreign availability of cryptographic systems of strategic capability, namely, those capable of resisting concerted cryptanalytic attack; (ii) to limit foreign availability of cryptographic systems of sufficient strength to present a serious barrier to traffic selection or the development of standards that interfere with traffic selection by making the messages in broad classes of traffic (fax, for example) difficult to distinguish; and (iii) to use the export-control process as a mechanism for keeping track of commercially produced cryptosystems, whether U.S. or foreign, that NSA may at some time be called upon to break. [26]

III. OBJECTIONS BY THE BUSINESS COMMUNITY

{24} As one can imagine, businesses which desire to produce software featuring cryptography also, as a general rule, wish to export that software expanding their market as well as the amount of money they can make. It has only recently become an issue due to the fact that cryptography has not been practical or in much demand in the past. Prior to the last decade or so, encryption was almost exclusively relegated to the murky world of espionage and traffic analysis. Since then, the advent of cheaper processing power, increasing use of computer networks, and increasing production and export of software have pushed the issue of encryption export regulations into the mainstream of business technology. [27]

{25} Speculations about how much money is actually being lost by businesses due to export restrictions vary; some say six to nine billion dollars, [28] while others say that six to nine billion dollars is the total profit made by all software exports, of which presumably only a portion would have incorporated encryption; [29] the most lucid assessment comes from Electronic Frontier Foundation co-founder and cyberspace commentator John Perry Barlow: "[w]hile it's impossible to set a credible figure on what the loss might be, it's high." [30] This seems to be the more sensible take on the matter since numbers tend to get crunched around to the benefit of the person who happens to be crunching with a consistency that impairs credibility and, furthermore, when discussing what a policy should be it makes little sense to rely on the numbers of the past rather than projecting the numbers of the future which are likely to grow exponentially. [31]

{26} The software industry's incentive for wanting to remove export controls is clear, it wants to make money which is exactly what businesses are supposed to do. Despite the obvious nature of the incentive, their arguments in support of deregulation are fairly compelling.

{27} First, the export controls do not work. This is evidenced by the fact that foreign countries are getting encryption technology and manufacturing encryption products despite the controls. A study by the software industry reported that a total of 20 foreign countries are manufacturing 215 hardware,

software, and combination products that use encryption. Of these 215 products, 84 use the DES algorithm which was invented in the United States with the help of the NSA and which was subject to the export controls. [32] Furthermore, the law itself is frequently breached--cryptographic programs go out over networks, are carried out in laptops or secured telephones, or are sold to foreign nationals in U.S. software and computer stores. [33]

{28} Second, most other countries do not regulate encryption software which contributes to the ineffectiveness of U.S. controls and places U.S. companies at a disadvantage. [34] European countries have few restrictions on their software exports [35], especially Germany, France, and Switzerland. [36] Britain freely allows export of mass market encryption software as well as encryption software for use in banking; export of encryption software for military activities is, however, restricted. [37] Even Russia, the old cold war enemy, provides in its new constitution that governmental restrictions on the use of cryptography is forbidden. [38]

{29} As a result, U.S. companies fear that they will fall behind in what stands to be a large market. Based on one survey, one-third of software consumers said that "they specifically look for encryption capabilities when buying software and would consider purchasing foreign software otherwise less desirable if that software offered data security not available in a U.S. software program." [39] And, in fact, importation of strong cryptography is not illegal. [40] Taking action on the matter, the software industry has put pressure on the Clinton Administration to change the export laws they consider to be damaging, unreasonable, and unrealistic. [41]

{30} In response, the Clinton Administration has proposed Clipper, a plan by which the government would hold its own set of encryption keys "in escrow," thereby allowing it to decrypt communications when the need arises while still providing high strength encryption. The business community widely rejected the Clipper proposal, largely based upon the sound logic that it is doubtful whether foreigners would be eager to buy products which would allow the U.S. government to eavesdrop on them.

{31} Recently, the Clinton administration was proposing a liberalization of controls allowing exports of products with encryption keys of up to 64 bits (as opposed to the current de facto 40 bit restriction) [42] as long as the keys were placed in escrow. Companies indicated a possible interest in a system employing corporate key-escrow rather than government key-escrow. [43] Specifically, in August of 1995, executives from eight software manufacturers wrote a letter to Vice President Gore saying, "We request that the administration immediately adopt a policy that allows the export of strong cryptography with a commercial key escrow system that provides appropriate back-up access for individuals, corporations, and governments. This capability should be tied to data recovery or escrow centers managed by commercial organizations with access by government agencies supported through existing search warrant mechanisms." They also call for permission to export "generally available" software programs with data encryption capabilities employing DES or other algorithms with similar strengths. [44]

{32} Finally, there is concern that beyond crippling the encryption software industry specifically, the export laws are going a fair way toward dampening the growth of commerce in general. Sally Katzen, chair of the Information Infrastructure Task Force's (IITF) Privacy Working Group and its Security Issues Forum, said that people want "confidence that their privacy is respected, that their intellectual property rights are protected, and that their security is effective." Discussion in the forum indicated that a lack of confidence in the networks would be inspired by unease about security of credit ratings, bank accounts, contents of messages, and security in general. If people do not have confidence in the security of the network, the infrastructure will grow much more slowly if it grows at all. [45]

{33} The business community, therefore, stands with fair unity in opposition to the export restrictions

placed on encryption products. The opposition stems from the fact that the restrictions are costing businesses money now, are likely to cost them more money in the future, place them at a disadvantage to foreign competitors, do not seem to be doing the job which such restrictions were designed for, and seem to be unnecessarily hindering the growth of the GII if not jeopardizing it all together.

IV. THE CLIPPER PROPOSAL--STRONG, EXPORTABLE CRYPTOGRAPHY?

{34} In an apparent attempt to resolve the tension between the desire to use and export products with strong cryptographic capabilities and the desire to keep from aiding those who would wish ill to the United States of America, on April 16, 1993, the White House announced the Escrowed Encryption Initiative, "a voluntary program to improve security and privacy of telephone communications while meeting the legitimate needs of law enforcement." [46]

{35} The Escrowed Encryption Initiative put forth the Escrowed Encryption Standard (EES), a standard which uses the Skipjack algorithm and is incorporated into the Clipper chip which possesses the key escrow feature. The Skipjack algorithm is to remain classified, ostensibly to enhance its security. [47]

{36} EES works as follows: If two people wish to communicate (for instance by telephone) with EES secured transmissions, both must have a phone equipped with the Clipper chip. The devices establish an 80-bit "session key" and pass this to their chips which, in turn, encrypt the session key with the device-unique key. Each device-unique key has an associated chip identification. Both the chip identification and the encrypted session key are placed in a Law Enforcement Access Field (LEAF). The LEAF is sort of an identification tag that accompanies the encrypted data of the rest of the stream of communication. [48] As was mentioned, every Clipper chip has a device-unique key; upon manufacture, a copy of that key is split into two components each of which is given to a separate governmental escrow agent. [49] Users of Clipper do not need to be aware of any of these details, they simply use their phones as always. [50]

{37} In order to decrypt a message, communications must be passed through a decrypt processor by law enforcement officials in order to determine whether or not they are Clipper communications, and, if so, what the chip identification is. Next, law enforcement officials must request the device unique key associated with the chip identification from the two escrow agents possessing the parts of the device unique key. Third, the device unique key is used to decrypt the session key located in the LEAF. Fourth, the session key is used to decrypt the body of the message. [51]

{38} In addition to the primary purpose of allowing law enforcement officials access to encrypted conversations, Clipper advocates suggest that it would have other beneficial uses. Individuals and businesses would have a way to retrieve data should they happen to lose their key. Also offered as a boon of Clipper is the ability of employers to crack the encryption of employees when those employees are using company computers and networks in order to embezzle or commit fraud. [52]

{39} Of course these "extras" of Clipper point to a disturbing question. What exactly are the standards by which people are to be able to obtain the keys. If, as was suggested, businesses can obtain keys to retrieve data, it is clear that a warrant is not strictly and without exception required in order to obtain the key. This is, in fact indicated by the language of the Clipper proposal where it said that in order to obtain keys from escrow agents, law enforcement agencies need to present evidence of "lawful authority." In all, the government has been evasive about questions as to who will have access to the ability to eavesdrop and as to precisely what constitutes "lawful authority." [53]

{40} In fact, there were many concerns about Clipper raised by the Digital Privacy and Security

Working Group, a group including DEC, Hewlett-Packard, IBM, Sun, MCI, Microsoft, Apple, and AT&T. Some of the questions sent to the White House by the Working Group were:

- Who would the escrow agents be?
- What are Clipper's likely economic impacts, especially in regard to export of American digital products?
- Why is its encryption algorithm secret and why should the public have confidence in a government-derived algorithm that can't be privately tested?
- Why is Clipper/Skipjack being ram-rodded into adoption as a government standard before completion of an over-all review of U.S. policies on cryptography?
- Why are the NSA, FBI, and NIST stone-walling Freedom of Information inquiries about Clipper/Skipjack? (In fact, NSA's response has been, essentially, "So? Sue us.")
- Assuming Clipper/Skipjack becomes a standard, what happens if the escrow depositories are compromised?
- Wouldn't these depositories also become targets of opportunity for any criminal or terrorist organization that wanted to disrupt U.S. law enforcement?
- Since the chip transmits its serial number at the beginning of each connection, why wouldn't it render its owner's activities highly visible through traffic analysis (for which government needs no warrant)?
- Why would a foreign customer buy a device that exposed his conversations to examination by the government of the United States?
- Does the deployment and use of the chip possibly violate the 1st, 4th, and 5th Amendments to the U.S. Constitution?
- In its discussions of Clipper/Skipjack, the government often uses the phrase "lawfully authorized electronic surveillance." What, exactly, do they mean by this?
- Is it appropriate to insert classified technology into either the public communications network or into the general suite of public technology standards? [54]

{41} Apparently, the White House was not particularly responsive to the questions. Barlow, co-founder of the Electronic Frontier Foundation (EFF) which was one of the members of the working group, describes the responses as follows:

- > Still unnamed, undescribed, and increasingly unimaginable were the escrow agents. Questions about the inviolability of the depositories were met with something like, "don't worry, they'll be secure. Trust us." There seemed a lot of that in Podesta's responses. While the government had convened a panel of learned cryptologists to examine the classified Skipjack algorithm, it had failed to inspire much confidence among the crypto establishment, most of whom were disinclined to trust anything they couldn't wack at themsleves. At the least, most people felt a proper examination would take longer than the month or so the panel got. After all, it took fifteen years to find a hairline fissure in DES. But neither Podesta (the White House spokesperson) nor any other official explained why it had seemed necessary to use a classified military algorithm for civilian purposes. Nor were the potential economic impacts addressed. Nor were the concerns about traffic analysis laid to rest. [55]

{42} Met with questions of this nature and widespread objections by those who were supposed to embrace Clipper, the government withdrew from the melee, at least for a little while. As noted above, as of the fall of 1995, the government has resumed its key-escrow advances with discussions with the software industry reminding it that key-escrowed products would be easily exportable and also at least listening to suggestions of a corporate escrow system. As yet, no new action has been taken. [56]

V. PRETTY GOOD PROTECTION AND PRETTY SERIOUS PROBLEMS

{43} Quite a bit of controversy has arisen from an RSA-based, public-key encryption program called PGP (short for Pretty Good Protection) written by Phil Zimmermann. Zimmermann wrote the program in response to Federal threats to crack down on the distribution of encryption software. [57] It was subsequently uploaded to the Internet by Kelly Goen in May of 1991, making it widely available in the United States and accessible from other nations. Then, in 1993, Assistant U.S. Attorney Bill Keane initiated an investigation based on possible charges of illegal exportation of a munition. [58] In furtherance of its investigation, a federal grand jury in San Jose, California issued subpoenas to Viacrypt and Austin Code Works, two companies involved in the production and distribution of commercial PGP, requiring them to supply all correspondence and records related to the international distribution of PGP. Both companies assert that they have no plans to sell their products internationally. [59]

{44} The case raises the issue of what constitutes an export. Zimmermann created the program because he wanted to make privacy an option for individuals using computer networks and related technologies, on the other hand, he did not upload the program to the Internet himself. And, even if he were responsible for the uploading, it is difficult to say whether uploading a product to the Internet constitutes an export. After all, the program still resides in a computer within the United States. Nevertheless, it is surpassingly easy for someone in another country to access Internet sites and bring PGP into their country, thereby moving strong encryption across borders. A major problem with holding persons liable for export violations when they upload encryption products to the Internet is that it would deny citizens of the United States an extremely efficient way of obtaining high quality encryption, something no one has seriously proposed outlawing yet.

CONCLUSION

{45} In the pursuit of Cold War objectives, the United States adopted a policy of limiting the exports of products it considered militarily dangerous for hostile nations to possess. Among these were encryption techniques and products. Until recently, however, this was of practically no interest to anyone except governments of sovereign nations engaged in the games that they play. However, with the advent of cheap and widespread computer processing power linked to communications networks, encryption technology has become of great interest to computer users and the companies who would supply them.

{46} In the course of hunting profit, U.S. businesses have requested that the government either eliminate or modify the export bans on encryption software. In favor of this position, they have pointed out that the encryption restrictions are largely ineffectual. Despite the restrictions, businesses of foreign nations are engaged in a robust trade of a wide variety of encryption products, many of which use techniques which are still restricted by the munitions laws. Furthermore, the laws are likely to become even more ineffectual as the communications networks expand, and the genie will escape from the bottle with more and more frequency.

{47} Other countries do not employ much in the way of encryption bans themselves. This demonstrates the viability of lacking encryption export controls while still keeping the national security viable as well as suggesting a grave potential for U.S. companies losing their edge in the market. What is more, the export restrictions tend to hinder the establishment of a standard by which commerce can be conducted internationally over the GII. Until such a standard is established, confidence in network security will be limited and full advantage will not be taken of the money making potential of the Information Infrastructure.

{48} In an inadequate attempt to resolve the tension between businesses' need for security and the

government's unease with the concept of not being able to eavesdrop when it feels it needs to, the Clinton Administration proposed Clipper despite the fact that it has serious flaws. First, it is incredibly unlikely to answer the export concerns of U.S. business. Foreigners would be of questionable intelligence were they content to employ encryption techniques which let the U.S. government listen without detection. Second, if Clipper is truly voluntary, U.S. citizens are unlikely to employ Clipper encryption since, as Barlow put it, "trusting the government with your privacy is like having a Peeping Tom install your window blinds." [60]

{49} The export controls on encryption start to make more sense if one takes a look at them from a slightly more paranoid perspective. Since the controls do not seem to be doing any appreciable degree of good as far as keeping encryption out of the hands of foreigners, it makes sense to look at the other side of the coin; what are export controls doing to keep encryption out of the hands of U.S. citizens?

{50} When PGP, an encryption program the U.S. government has a good deal of trouble cracking, was made widely available to U.S. citizens via the Internet, the U.S. government began to come down on its creator, an action surely likely to inhibit other would-be providers of high quality encryption. At approximately the same time, the government announces Clipper, a system designed to give domestic law enforcement officials and espionage agencies alike access to private communications. Meanwhile, the export controls continue to chill U.S. companies' development and sales of high quality encryption by making it more efficient to "dumb-down" their encryption capabilities in order to be able to sell one product both domestically as well as abroad.

{51} In crafting policies and in deciding which laws to propose, which laws to keep, and which laws to do away with, lawmakers, businesses, public interest groups, and everybody else for that matter, would be well advised to attempt to raise their head out of the muck and their day to day concerns and consider a bigger picture, particularly with regard to the digital technologies and how they change the rules of day to day concerns..

{52} One consideration is the design of the Internet and similar networks. Originally the Department of Defense was searching for a communications mechanism which would maintain the communication flow in the event of a nuclear strike which destroyed major communications hubs. The answer, essentially, was to create a web which routed information around troubled spots. Looked at in one way, encryption restrictions could be viewed as a communication trouble spot. This could produce at least two outcomes. First, the restrictions are simply by-passed, encryption flows around them, getting it to everyone who wants it. This would suggest that the law is impotent, create a glaring inequity in the relatively rare instances where the law is enforced, and generally contribute to an unhealthy disrespect for the law. Or second, the U.S. government is so successful at sealing off the country that encryption does not get out of the country. However, this could make the entire nation a sort of trouble spot in the network causing information to route around it. This is not to say that information ceases to come into the country necessarily, only that the volume decreases. For example, it could be the result that only information that needs to be secure has the tendency to route around the United States since our high quality encryption is incompatible or at least it takes more work to make it compatible and, therefore, safety and efficiency dictate that transmissions be routed around the United States.

{53} Whatever the exact effects of such an avoidance, they are unlikely to be desirable for the health of either the economy of or the free flow of information within the United States. Another concern is the relative danger of erring on the side of privacy verses that of erring on the side of authority. While dashing headlong into the grip of technology which is not fully understood, indeed which possibly cannot be understood without first experiencing it (and even then maybe not), we are bound to make mistakes. The hazards of unchecked privacy are much like ogres, witches, and monsters under the bed; decidedly fierce, but hard to point to definitively because they are rarely if ever seen. The hazards of

increased governmental control, on the other hand, have been seen in every age of humanity. The prudent course would be to err on the side of privacy since, if the costs outweigh the benefits, the forces of authority can be counted upon to gather power into their hands. It is doubtful whether the forces of privacy could be counted upon to successfully remove power from the side of authority were the positions reversed.

{54} A final concern to be noted (at least for the purposes of this paper) is the bias of the network. Two of a digital network's tendencies are to replicate data and to spread it widely. Ultimately, these tendencies will probably prove insurmountable by those who would desire to keep information between themselves and one or few others (though the person wishing to keep information to himself should still prove successful). [61] However, encryption could at least prove to be a stalling tactic to prevent total disclosure until our society is at least a bit more ready for it. This means that encryption would make it so that the original information is only in a readable form in the receiver's and possibly the sender's systems; though the receiver would find it easy to transmit the information where he would. At the very least, encryption would prevent the information from lying dormant in a useful form in any computer the message happened to have bounced through between sender and receiver. However, it is doubtful that, in the long run, encryption will prove an effective adversary of the digital network's ability and tendency to replicate and distribute information. In order to read information, the human receiver has to be able to decrypt that information and, once decrypted, it can be sent anywhere. It will be hard to know which information has been safely destroyed and which information has been scattered into the network. So perhaps, and this is nearly unadulterated speculation, our privacy will revert to almost as little as we had in the tribal village; but, maybe encryption can battle this tendency until we are more used to the idea and its implications.

{55} In conclusion, therefore, the laws restricting the export of high quality encryption may once have served its stated and legitimate purpose of enhancing U.S. security, but due to the replicative nature of software, the increased volume of commerce, and the wide availability of substantial computing power, it is no longer feasible to keep encryption out of the hands of entities powerful enough to be considered a foreign threat to the United States. Since the laws are not working for their stated purposes, it would be distasteful in the extreme to maintain them for the unsavory purpose of keeping high quality encryption out of the possession of U.S. citizens without at least having the courtesy to notify them of that policy. The United States government has enough problems without cheapening its credibility any further than has already been done. Whatever the reasons for maintaining the restrictions, they have the effect of putting U.S. companies at a disadvantage in an expanding and important market which is likely to grow in coming years. Furthermore, restricting high quality encryption has the effect of hampering the GII, an artifact which is likely to provide the engine of considerable economic activity. To say the least, it is a strange course of action to be followed by a country whose business, as Calvin Coolidge once said, is business.

Endnotes

[1] Douglas J. Masson; B.A. Miami University 1993; J.D. Indiana University 1996; I would like to thank Professor Fred Cate for showing me how to decide what the law is and Professor Harmeet Sawhney for showing me how to decide what the law should be.

[2] Ira S. Rubenstein, Export Controls on Encryption Software in Coping with U.S. Export Controls: 1994; 705 PLI/Comm 177, sec. 2(a), (Practising Law Institute Commercial Law and Practice Course Handbook Series 1994).

[3] Id. at sec. 2(c) fn. 4.

[4] Id. at sec. 2(b).

[5] Some Beltway wags have been heard to comment that NSA stood for "No Such Agency" due to the mystery in which it has been veiled. John Perry Barlow, Decrypting the Puzzle Palace, Communications of the ACM, July 1992 at 25. For a detailed discussion of the NSA, see James Bamford, The Puzzle Palace (1982), a book which, rumor has it, interns of the NSA were instructed to not to read which is, one supposes, much like telling a person not to think of those ubiquitous pink elephants.

[6] Rubenstein, supra note 1, at sec. 2(c).

[7] Id. at sec. 2(c).

[8] Id. at sec. 2(b).

[9] Id. at sec. 2(c).

[10] See id. at sec. 3 (citing 22 CFR sec. 120.3).

[11] See Rochelle M. Tarlowe, Deregulating Dual-Use Exports to Russia: Is U.S. National Security at Risk?" 18 Fordham Int'l L.J. 959 (1995).

[12] Rubenstein, supra note 1, at sec. 3 (citing 22 CFR secs. 120-130 and noting that the legislative authority for the ITAR is sec. 38 of the Arms Export Control Act, as amended, Pub. L. No. 90-629, 82 Stat. 1320 (codified at 22 USC sec. 2778)).

[13] Id. at sec. 3 (quoting 22 CFR sec. 121.1, Category XIII(b), as amended by 57 Fed. Reg. 15227 (Apr. 27, 1992)).

[14] Id. at sec. 3 (citing 22 CFR sec. 125.1(a)). Despite plausible readings to the contrary, it has been made clear that the public domain exception only applies to information, not to software. See id. at sec. 3 (citing 22 CFR sec. 120.10).

[15] Charles L. Evans, Comment, U.S. Export Control of Encryption Software: Efforts to Protect National Security Threaten the U.S. Software Industry's Ability to Compete in Foreign Markets, N.C.J. Int'l L. & Com. Reg. 469.

[16] Rubenstein, supra note 1, at sec. 3(b)(4) (citing 22 CFR sec. 136.1(a)).

[17] See id at sec. 3(b).

[18] Id. at sec. 3(b)(1).

[19] Evans, supra note 14 (citing 22 CFR sec. 121.1 Category XIII(b)(1)).

[20] Rubenstein, supra note 1, at sec. 3(b)(2).

[21] Id. at sec. 3(b)(3) (citing James LeMunyon, Deputy Assistant Secretary of Export Administration in Unpublished Bureau of Export Administration document entitled Commerce-State Memo on

Cryptographic Items, August 11, 1989 copy in Rubenstein's possession. Suggesting that one sees also, Transfer of Encryption Software and Devices, OEL Insider, 6-7 (Dec. 1989)).

[22] Rubenstein, supra note 1, at sec. 3(b)(3).

[23] Id. at 3(c).

[24] 22 USC sec. 2778(c) (1988).

[25] 50 USC sec. 2410(c) (1988).

[26] Susan Landau, Codes Keys and Conflicts: Issues in U.S. Crypto Policy, Report of a Special Panel of the ACM U.S. Public Policy Committee 25, (June 1994).

[27] Rubenstein, supra note 1, at sec. 1.

[28] U.S. Software Companies Competitiveness Threatened by Outdated Export Regulations, $6 to $9 Billion in Annual Revenues at Risk, Business Wire, Oct. 12, 1993.

[29] See Evans, supra note 14, at fn. 138-41.

[30] Barlow, Decrypting the Puzzle Palace, supra note 4.

[31] See Susan Landau, Codes Keys and Conflicts: Issues in U.S. Crypto Policy, Report of a Special Panel of the ACM U.S. Public Policy Committee 13, (June 1994). On the other hand, the report notes that cryptography remains a niche market in which only a handful of companies gross a few tens of millions of dollars even though cryptography supporters have been predicting an explosion for the last twenty years. Nevertheless, it notes, arguments in favor of cryptography's importance and bright future remain: "the cost of cryptography is declining, information products have become a major industry, and the popularity of (vulnerable) wireless communications is increasing." Id.

[32] New SPA Study: Export Regulations Preclude U.S. Companies from Cashing in on Multi-Million Dollar Encryption Software Market, U.S. Newswire, Sept. 1, 1993, available in LEXIS, News Library, USNWR File.

[33] Peter H. Lewis, Multinational Businesses Hamstrung by Security Laws; Security Export Law Puts Some Businessmen in a Bind, The Austin American-Statesman, April 17, 1995.

[34] See Evelyn Richards, U.S. Plan to Restrict Encryption Software Exports Draws Protests, Wash. Post, Nov. 14, 1991, at B11.

[35] Id.

[36] Evans, supra note 14, at Part V(B).

[37] Id.

[38] John Perry Barlow, A Plain Text on Crypto Policy, Communications of the ACM, Nov. 1993, at 21, 24.

[39] U.S. Software Companies Competitiveness Threatened by Outdated Export Regulations, $6 to $9 Billion in Annual Revenues at Risk, Business Wire, Oct. 12, 1993.

[40] Charlotte Dunlap, Technology Trends--Internet Security; The Politics of Electronic Commerce, Computer Reseller News, September 11, 1995.

[41] U.S. Software Companies Competitiveness Threatened by Outdated Export Regulations, $6 to $9 Billion in Annual Revenues at Risk, Business Wire, Oct. 12, 1993.

[42] Dunlap, supra note 37.

[43] U.S. Announces Plan to Lift Curbs on Exports of Some Encrypted Software, BNA International Trade Reporter, Aug. 23, 1995.

[44] Id.

[45] Technical Standards, Trade Barriers, Security Concerns Pose Barriers to Growth of Global Information Infrastructure, BNA Management Briefing, Communications.

[46] Landau, supra note 25, at 47.

[47] Barlow, A Plain Text on Crypto, supra note 37. Some cryptography experts along with others are critical of the prudence of using a publicly untested classified algorithm. The algorithm was tested to a degree by a panel of cryptography and security experts and it appeared to be strong and resistant to attack, however the testing was limited in both scope and in time. It has been suggested, therefore, that Skipjack could contain flaws that are not immediately obvious, and, for the more paranoid, even a governmentally inserted "trapdoor" which would allow the government to circumvent any safeguards. See Landau, supra note 25 at 50.

[48] Dorothy E. Denning, The Case for 'Clipper:' Clipper Allows Escrowed Encryption, Technology Review (July 1995), at 48.

[49] The two escrow agents are the National Institutes of Standards and Technology (NIST) and the Department of the Treasury under the Federal Data Processing Standard. The Federal Data Processing Standard is a toned down version of the EES under which the government ordered 50,000 Clipper devices and under which Clipper is being kept alive after the EES was rejected by businesses and privacy advocates. John Perry Barlow, Jackboots on the Infobahn, Wired 2.04 (April 1994).

[50] Denning, supra note 46.

[51] Id.

[52] Id.

[53] Barlow, A Plain Text on Crypto Policy, supra note 37.

[54] Id.

[55] Id.

[56] See note 42 and accompanying text. This resurgence has been dubbed "Son of Clipper."

[57] John Markoff, Federal Inquiry on Software Examines Privacy Programs, New York Times, September 21, 1993.

[58] Who Said the Government Isn't Responsive, available at http://www.eff.org/pub/Legal/cases/PGP_Zimmermann/gov_access.article.

[59] Markoff, supra note 56.

[60] Barlow, Jackboots on the Infobahn, supra note 48.

[61] Once again proving the wisdom of Benjamin Franklin's old saw about three men keeping a secret being successful only if the other two are dead.
